REMARKS

Claims 1-20 are pending and stand rejected. In response, claims 11, 4, 6, 9, 10, 13, 14, 15, 16, 19, and 20 are amended, claim 2 is canceled, and claim 21 is added. Claims 1 and 3-21 are pending upon entry of this amendment.

Double Patenting Rejection

Claims 1-3 and 6-12 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 10-27 of copending application No. 10/632,857. The Examiner asserts that the two sets of claims are not patententably distinct because they both disclose "categories of data, removal of literal field data, flagging suspicious commands that are being audited in real time, and use of a training phase to monitor code." While the Examiner acknowledges there are differences between the claim sets, the Examiner asserts that these differences would have been obvious to a person of ordinary skill in the art.

Applicants respectfully traverse this rejection. Claims 10-27 of the '857 application are *dependent* claims that incorporate the limitations of claim 1. Claim 1 of the '857 application recites "generating retrieval information characteristic of data sent to a retriever" and "accessing at least one rule using…retrieval information." Thus, the claims of the '857 application describe analyzing data retrieved from a database or other computer code in response to a command. The claims of the instant application, in contrast, relate to observing commands that are sent to the database.

The two sets of claims are quite different, and the Examiner has not performed the analysis required by MPEP 804.II.B to explain why these differences would be obvious. The rejection does not accurately describe the differences between the inventions defined by the conflicting claims because it fails to consider the elements found in claim 1 of the '857 application. Also, the reasons given as to why a person of ordinary skill in the art would consider the claims obvious are merely cursory statements without any supporting analysis. For these reasons, Applicants respectfully request that the Examiner withdraw the double patenting rejection.

35 U.S.C. § 112 Rejection

Claim 4 stands rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, it is unclear whether "one command" in line 1 refers to "commands that are accessing" from claim 1, line 4, or "acceptable commands" from claim 1, line 7.

In response, Applicants have amended claim 4 to state "one observed command." "Observed" references the "observing" step of claim 1 that introduces the "commands that are accessing." Therefore, Applicants submit that claim 4 now clearly recites that the command is one of the "commands that are accessing" from claim 1.

35 U.S.C. § 103 Rejections

Claims 1-6, 8-17, and 19-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Desai et al., US 2003/0188189 in view of Harkins, US 6,775,827. Further, claims 7 and 18 stand rejected under § 103(a) as being unpatentable over Desai and Harkins and further in view of Pandit et al., US 2003/0154402. Applicants respectfully traverse the § 103 rejections.

Applicants have amended the claims to clarify that the "computer code" referenced therein is a database. This feature was previously recited by canceled claim 2. Generally, the amended claims describe training a database intrusion detection system in real time. Independent claims 1 and 16, for example, recite:

> observing, in real time, commands that are accessing the database; and
> deriving from said commands, in real time, a set of acceptable commands.

Thus, the claimed invention observes commands that are accessing a database and derives, from those commands, a set of acceptable commands. Claim 20 recites the observing and deriving elements, and further recites comparing commands received during an operational phase with the set of acceptable commands. Claim 21 recites elements similar to those found in other independent claims.

In order to establish a prima facie case of obviousness, the Examiner must show (i) some suggestion or motivation, either in the references themselves or based on knowledge of one of ordinary skill in the art, to modify the reference or to combine reference teachings, (ii) a reasonable expectation of success, and (iii) that the references when

combined teach or suggest all the claim limitations. See MPEP § 2143. This burden has not been met.

In the rejection of claim 2, the Examiner asserts that Desai discloses a database intrusion detection system at paragraphs [0052] and [0056]. Desai discloses an intrusion detection and response system that analyzes received data to identify normal and abnormal data traffic patterns. While Desai broadly discusses detecting attacks on network hosts, Desai never specifically discusses database intrusion attacks. For example, at [0092] Desai describes examples of threats it can detect, but does not mention database intrusion detections.

Further, the portions of Desai relied upon by the Examiner do not disclose a database intrusion detection system. Paragraph [0052] describes an "attack signature database" that holds data describing known attack signatures. However, Desai neither discloses nor suggests monitoring for attacks on this database. Paragraph [0056] mentions monitoring SQL traffic for abnormal behavior, but provides no teaching or suggestion of how to detect database intrusions based on this monitoring.

Indeed, the Examiner acknowledges that Desai fails to disclose either the "observing" or "deriving" elements of claim 1 but maintains that these deficiencies are remedied by Harkins. Harkins does not disclose a database intrusion detection system. Rather, Harkins discloses an automated method for generating an audit record of a computer program for debugging purposes. At col., 4, lines 13-17, Harkins describes how its method provides real-time analysis of an executing program but does not teach or suggest that the executing program is accessing a database. Therefore, Harkins does not teach or suggest "observing…commands that are accessing [a] database" as claimed.

At col. 5, lines 41-49, Harkins discloses that it uses default initial execution profiles that provide frequently selected audit execution options. These profiles describe the execution options for the program being debugged. The Examiner asserts that the execution profiles contain frequently selected commands and are thus similar to a set of acceptable commands. However, the execution profiles are utilized to detect faults in programs; the fact that an execution profile is frequently selected does not imply that any commands in the profile are acceptable. Rather, the commands are merely used to understand the operation of the program being debugged.

In the rejection of claim 13, 19, and 20, the Examiner asserts that "comparing commands that access the database during an operation phase with commands in the set of acceptable commands" (quoting from claim 20) is shown in Harkins at col. 2, lines 56-58. These portions describe configuration records that are compared by showing the differences between two builds of the program being debugged. Harkins neither discloses nor suggests the comparing element recited by the claims.

Further, there is no reason why a person of ordinary skill in the art would be motivated to combine Desai and Harkins to create a database intrusion detection system. Neither reference shows a database intrusion detection system per se. Desai describes a generic intrusion detection system that monitors traffic on a network. In contrast, Harkins describes a software development tool that is embedded within a single program being debugged. A person considering the problem of monitoring network traffic for database intrusions would not be motivated to consider program debugging art, and neither reference suggests such a combination. In addition, there is no reason to believe the references could be successfully combined given the disparate nature of the technology. The Examiner's statements supporting the combination are conclusory and at best rely on hindsight reasoning.

Pandit, upon which the Examiner relies for the rejection of claims 7 and 18, fails to remedy the deficiencies of Desai and Harkins. Pandit discloses a system and method for storing events to enhance intrusion detection. While Pandit describes storing events in a database, it neither teaches nor suggests that the stored events describe database intrusion detections. Accordingly, Pandit does not disclose or suggest stripping literal field data from database access commands as claimed.

Claim 4 recites that a command is from a group of certain commands. The Examiner asserts that this element is found in paragraphs [0052] and [0092] of Desai, but in fact these paragraphs do not describe the claimed commands.

For the above reasons, Applicants respectfully submit that claim 4 satisfies § 112, and that a person of ordinary skill in the art, considering the teachings of Desai, Harkins, and Pandit, either alone or in combination, would find the invention recited by claims 1, 4, 16, and 20-21 obvious. Those claims not specifically mentioned above incorporate the features of their base claims and are allowable for at least the same reasons. Therefore, Applicants respectfully request that the application be passed to issue.

The Examiner is invited to contact the undersigned to advance the prosecution of this application.

Respectfully submitted,

CAREY NACHENBERG ET AL.

Dated: October 19, 2006

By: /Brian Hoffman/
Brian M. Hoffman, Reg. No. 39, 713
Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax: (415) 281-1350